

**ALBRIGHT, STODDARD, WARNICK &  
ALBRIGHT**

G. MARK ALBRIGHT, ESQ.

Nevada Bar No. 1394

KYLE W. FENTON, ESQ.

Nevada Bar No. 16235

801 South Rancho Drive, Suite D-4

Las Vegas, Nevada 89106

Telephone: (702) 384-7111

Facsimile: (702) 384-0605

Email: [gma@albrightstoddard.com](mailto:gma@albrightstoddard.com)

[kfenton@albrightstoddard.com](mailto:kfenton@albrightstoddard.com)

[Additional Counsel Listed on Signature Page]

*Attorneys for Plaintiff Ronald Hansen and the  
Proposed Classes*

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

RONALD HANSEN, on behalf of himself and all  
others similarly situated,

Plaintiff,

v.

RIVERSIDE RESORT AND CASINO, LLC, a  
and RIVERSIDE RESORT AND CASINO, INC.,

Defendants.

Case No.

**PLAINTIFF'S CLASS ACTION  
COMPLAINT & JURY DEMAND**

Plaintiff Ronald Hansen, by and through his counsel, brings this Class Action Complaint against Defendants Riverside Resort and Casino LLC and Riverside Resort and Casino, Inc. (collectively "Defendants" or "Riverside"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

**I. NATURE OF THE ACTION**

1. Plaintiff brings this class action against Defendants for failure to properly secure and safeguard sensitive information that Plaintiff and other Class Members, as current and former

1 customers of Riverside, entrusted to it, including, without limitation, and upon information and  
2 belief, their names and Social Security numbers (collectively, “personally identifiable information”  
3 or “PII”).

4 2. Defendants own and/or operate a well-known casino, hotel and resort complex in  
5 Laughlin, Nevada including more than 1,400 guestrooms, a dozen restaurants and bars, a 2,650-seat  
6 concert venue, a movie theater, a 34-lane bowling alley and a casino gaming floor with over 1,200  
7 slot machines, two dozen tables, a poker room, and a sportsbook.

8  
9 3. Plaintiff and Class Members are current and former customers of Riverside.

10 4. As a condition of being customers of Riverside and receiving its products and services,  
11 Plaintiff and other Class member were and are required to entrust Riverside with this highly sensitive  
12 PII, including but not limited to, their names and Social Security numbers, driver’s license numbers,  
13 and/or financial account information.

14 5. Plaintiff and Class Members provided their PII to Riverside with the legitimate and  
15 reasonable expectation, and on the mutual understanding, that Riverside would comply with its  
16 obligations to keep that information safe, confidential and secure from unauthorized access.

17  
18 6. Riverside derives a substantial economic benefit from collecting, retaining and/or  
19 storing Plaintiff’s and other Class Members’ PII. Without it, Riverside could not perform the services  
20 that it provides to customers or remain in business as a hotel resort and casino.

21 7. Riverside had a duty to adopt reasonable measures to protect the PII of the Plaintiff and  
22 other Class Members from unauthorized or involuntary disclosure to third parties and to audit,  
23 monitor, and verify the integrity of its network and systems, as well as its vendors and affiliates, for  
24 their own cybersecurity, to comply with its legal duties to keep consumers’ PII safe, secure and  
25 confidential.

26  
27 8. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and other Class  
28 Members’ PII, Riverside assumed legal and equitable duties to ensure the protection of that PII, and

1 it knew or should have known that it was thus responsible for protecting Plaintiff's and other Class  
2 Members' PII from disclosure.

3 9. On or about September 5, 2024, Riverside began informing state attorneys general and  
4 impacted consumers that it had detected a data breach (the "Data Breach"). Plaintiff and other Class  
5 Members received notice letters (the "Notice") dated September 5, 2024, disclosing that "[o]n July  
6 25, 2024, Riverside learned of suspicious activity in its environment" and "immediately engaged  
7 forensic specialists in cybersecurity and data privacy to investigate further."

8  
9 10. Riverside's Notice letters did not specify how many individuals were affected by the  
10 Data Breach or provide details about the circumstances surrounding the Data Breach. However, news  
11 outlets have reported that Riverside had "confirmed a data breach that leaked confidential information  
12 on more than [55,000] customers."<sup>1</sup>

13 11. According to the Notice sent to Plaintiff and other Class Members, Riverside then  
14 "determined that an unauthorized third party potentially accessed and acquired certain files during  
15 this incident." Riverside "then performed an extensive and comprehensive review of the data to  
16 identify what personal information may have been impacted in this incident, On August 9, 2024,  
17 Riverside "identified the persons whose sensitive information was potentially impacted," and  
18 Riverside claims that it then "promptly disabled all relevant accounts and worked with our third-party  
19 specialists to confirm the security of our environment."  
20

21 12. As a result of the Data Breach, Plaintiff and the other Class Members thus not only lost  
22 the confidentiality and security of their PII, they lost access to their Riverside accounts.  
23

24 13. Upon information and belief, Plaintiff's and Class Members' PII has been exposed and  
25 exfiltrated as a result of this Data Breach. Noticeably absent from the Notice letters is the lack of any  
26

---

27 <sup>1</sup> E.g., Casino.org, 9-13-2024 "*Laughlin's Riverside Resort Casino Confirms Data Breach, 55K*  
28 *Customers Affected*"; at <https://www.casino.org/news/laughlins-riverside-resort-casino-confirms-data-breach/> (last accessed Sept. 24, 2024).

1 real discussion of the specifics of the root cause of the Data Breach, the vulnerabilities that were  
 2 exploited, and the remedial measures that were or are being undertaken to ensure such a breach does  
 3 not happen again. To date, these critical facts have not been explained or clarified to Plaintiff or the  
 4 other Class Members, who have a vested interest in ensuring that their PII remains secure and  
 5 protected going forward.

6 14. The attacker accessed and acquired files that Riverside stored on its systems containing  
 7 unencrypted PII of the Plaintiff and other Class Members, including but not limited to their Social  
 8 Security numbers.  
 9

10 15. While Defendants offered relatively little specific information about the incident in  
 11 their September 5, 2024 Notices to Plaintiff and other Class Members, news outlets and other sources  
 12 reported (even before Riverside's Notices) that the Breach was a ransomware attack by a relatively  
 13 new but already "notorious Lynx group," described as a "double-extortion ransomware group that  
 14 emerged in August [2024]"<sup>2</sup> "known for targeting multiple sectors while avoiding government,  
 15 healthcare, and non-profits", and "distinguishes itself by encrypting files and stealing data,  
 16 demanding ransom payments through TOR"<sup>3</sup>. Their attacks are sophisticated, often leveraging  
 17 behavior-based, file-based, and machine learning-based detection methods to evade security  
 18 measures."  
 19

20 16. Plaintiff brings this action on behalf of all persons whose PII was compromised as a  
 21  
 22

---

23 <sup>2</sup> Halycon, *Ransomware News*, Aug. 30, 2024, *Riverside Resort Casino in Laughlin Hit by Lynx*  
 24 *Ransomware Attack*, at <https://ransomwareattacks.halcyon.ai/attacks/riverside-resort-casino-in-laughlin-hit-by-lynx-ransomware-attack> (last accessed Sept. 25, 2024).

25 <sup>3</sup> "The Onion Router," a free software platform "designed to protect users' identities while they are  
 26 browsing the Internet and exchanging messages. Tor is widely called the largest anonymity network."  
 27 (at <https://www.britannica.com/technology/Tor-encryption-network> ) (last accessed Sept. 24, 2024).  
 28

1 result of Riverside's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn  
 2 Plaintiff and Class Members of Riverside's inadequate information security practices; and (iii)  
 3 effectively secure hardware and software containing protected PII using reasonable and effective  
 4 security procedures free of vulnerabilities and incidents. Riverside's conduct amounts to, among other  
 5 things, negligence and violates state and federal statutes.

6 17. Plaintiff and Class Members have suffered material injury as a result of Defendants'  
 7 conduct. These injuries include:

- 8 (i) lost or diminished value of PII;
- 9 (ii) out-of-pocket expenses associated with travel expenses and the prevention,  
 10 detection, and recovery from identity theft, tax fraud, and/or unauthorized use  
 11 of their PII;
- 12 (iii) lost opportunity costs associated with attempting to mitigate the actual  
 13 consequences of the Data Breach, including but not limited to lost time;
- 14 (iv) the disclosure of their private information;
- 15 (v) loss of access to their money and financial accounts; and
- 16 (vi) the continued and certainly increased risk to their PII, which: (a) remains  
 17 unencrypted and available for unauthorized third parties to access and abuse;  
 18 and (b) may remain backed up in Defendants' possession and is subject to  
 19 further unauthorized disclosures so long as Defendant fails to undertake  
 20 appropriate and adequate measures to protect it.

21 18. Defendants have disregarded the rights of Plaintiff and Class Members by  
 22 intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and  
 23 reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded; failing  
 24 to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable,  
 25  
 26  
 27  
 28

1 required and appropriate protocols, policies and procedures regarding the encryption of data, even for  
2 internal use.

3 19. As a result, the PII of Plaintiff and Class Members was compromised through  
4 disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in  
5 ensuring that their information is and remains safe, and they should be entitled to injunctive and other  
6 equitable relief.

## 7 8 **II. PARTIES**

9 20. Plaintiff Ronald Hansen is, and at times relevant, has been a citizen of the United  
10 States and the State of Mississippi. Prior to moving to Mississippi, Plaintiff Hansen, including at  
11 times when he was a customer of Riverside, was a resident of the State of California. Plaintiff received  
12 a Notice letter from Riverside notifying him of the Data Breach on or around September 5, 2024.

13  
14 21. Defendants Riverside Resort and Casino, LLC, and Riverside Resort and Casino, Inc.  
15 own and/or operate a casino, hotel and resort complex in Laughlin, Nevada known as Don Laughlin's  
16 Riverside Resort Hotel & Casino, located at 1650 S Casino Dr, Laughlin, Nevada 89029. According  
17 to information from the Nevada Secretary of State's website, Riverside Resort and Casino, LLC is an  
18 active Nevada limited liability company formed on December 13, 2023 whose Manager is listed as  
19 Matthew C. Laughlin of 1650 S. Casino Drive, Pmb 500, Laughlin, Nevada, 89029; and Riverside  
20 Resort and Casino, Inc. is a Nevada corporation formed on June 11, 1974, with Mr. Laughlin listed  
21 as its Director, President and Treasurer at the same address. Defendants share a registered agent,  
22 Sierra Corporate Services - Las Vegas, 2300 West Sahara Ave., Ste. 1200, Las Vegas, Nevada, 89102.  
23

## 24 25 **III. JURISDICTION AND VENUE**

26 22. The Court has subject matter jurisdiction over this action under the Class Action Fairness  
27 Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and  
28 costs. The number of class members is over 100, many of whom reside outside the State of Nevada,

1 and have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C.  
2 §1332(d)(2)(A).

3 23. This Court has jurisdiction over Defendants because, among other things, they operate  
4 in this District, are incorporated in this District, and because have principal places of business and  
5 headquarters in this District.

6 24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) Because, among  
7 other things, a substantial part of the events giving rise to this action occurred in this District,  
8 Defendants have harmed Class Members residing in this District, and Defendants have its principal  
9 places of business and headquarters in this District.  
10

#### 11 **IV. FACTUAL BACKGROUND**

##### 12 **A. The Data Breach**

13 25. As outlined above, Riverside only recently disclosed that it learned two months ago, on  
14 July 25, 2024, that it had suffered a serious data security incident (the Breach) and that by August 9,  
15 2024 (six weeks ago) it had ascertained the identities of persons whose sensitive information was  
16 potentially impacted.  
17

18 26. Riverside appears to have waited nearly a month after identifying those potential  
19 victims to begin to notify state attorneys general and impacted consumers that it had the “Data  
20 Breach.” Plaintiff and other Class Members received Notice letters dated September 5, 2024,  
21 disclosing that “[o]n July 25, 2024, Riverside learned of suspicious activity in its environment” and  
22 “immediately engaged forensic specialists in cybersecurity and data privacy to investigate further.”  
23

24 27. According to the Notices, Riverside merely “determined that an unauthorized third  
25 party potentially accessed and acquired certain files during this incident” and “then performed an  
26 extensive and comprehensive review of the data to identify what personal information may have been  
27 impacted in this incident.” Riverside’s September 5, 2024 Notices did not specify how many  
28 individuals were affected by the Data Breach or provide any significant details about the

1 circumstances surrounding the Breach. However, news outlets have reported that Riverside had  
2 “confirmed a data breach that leaked confidential information on more than [55,000] customers.”<sup>4</sup>

3 28. By August 9, 2024, Riverside states that it had “identified the persons whose sensitive  
4 information was potentially impacted,” after which it claims to have “promptly disabled all relevant  
5 accounts and worked with our third-party specialists to confirm the security of our environment.”

6 29. Upon information and belief, Plaintiff’s and Class Members’ PII has been exposed and  
7 exfiltrated as a result of this Data Breach. Noticeably absent from the Notice letters is the lack of any  
8 real discussion of the specifics of the root cause of the Data Breach, the vulnerabilities that were  
9 exploited, or the remedial measures that were/are being undertaken to ensure such a breach does not  
10 happen again. To date, these critical facts have not been explained or clarified to Plaintiff or the other  
11 Class Members, despite their clear vested interest in ensuring that their PII remains safe and protected  
12 going forward.  
13

14 30. Upon information and belief, the attacker accessed and acquired files that Riverside  
15 stored on its networks and systems containing unencrypted PII of the Plaintiff and other Class  
16 Members, including at least their names and Social Security numbers.  
17

18 31. As noted above, Defendants provided relatively little specific information about the  
19 incident in their September 5, 2024 Notices to Plaintiff and other Class Members, but news outlets  
20 and other sources reported (even before Riverside’s Notices) that the Breach was a ransomware attack  
21 by a relatively new and sophisticated group of ransomware hackers known as Lynx.<sup>5</sup>  
22

23 32. halcyon’s *Ransomware News* outlet disclosed on August 30, 2024 that “[t]he Lynx  
24 ransomware group has claimed responsibility for the attack, asserting that they have infiltrated  
25

26 <sup>4</sup> E.g., Casino.org, 9-13-2024 “*Laughlin’s Riverside Resort Casino Confirms Data Breach, 55K*  
27 *Customers Affected*”; at [https://www.casino.org/news/laughlins-riverside-resort-casino-confirms-](https://www.casino.org/news/laughlins-riverside-resort-casino-confirms-data-breach/)  
28 [data-breach/](https://www.casino.org/news/laughlins-riverside-resort-casino-confirms-data-breach/) (last accessed Sept. 24, 2024).

<sup>5</sup> See *supra* at \_\_\_\_.

Riverside Resort's data systems" and had "posted sample screenshots on their dark web portal to substantiate their claims. The attack has reportedly led to the encryption of critical files, appended with a .LYNX extension, and the exfiltration of sensitive data." [6]

33. The *Ransomware News* report continued:

### Potential Vulnerabilities

Riverside Resort's extensive digital infrastructure, which includes online booking systems, customer databases, and financial transactions, makes it a lucrative target for ransomware groups like Lynx. The hospitality sector's reliance on continuous operations and customer trust further exacerbates the impact of such attacks, making robust cybersecurity measures imperative.

### Implications for the Hospitality Sector

This attack underscores the growing threat of ransomware in the hospitality industry. As establishments like Riverside Resort continue to expand their digital footprints, they must prioritize cybersecurity to protect against increasingly sophisticated cyber threats. [7]

34. According to halcyon's *Ransomware News* site, the Lynx group is responsible for at least 20 data breach attacks (including the Riverside incident) over the last two months or so.<sup>8</sup>

35. Another outlet, Comparitech, pointed out that Riverside's September 5, 2024 Notice did "not specify whether the data belonged to guests, employees, or a mix of both."<sup>9</sup>

36. Riverside had obligations to Plaintiff and to Class Members to safeguard their PII and protect it from unauthorized access and disclosure, including by ensuring that Riverside's vendors

---

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> <https://ransomwareattacks.halcyon.ai/threat-group/lynx>

<sup>9</sup> Comparitech, Paul Bischoff, Sept. 9, 2024, *Riverside Resort Hotel and Casino hit by ransomware attack, guest SSNs compromised*, at <https://www.comparitech.com/news/riverside-resort-hotel-and-casino-hit-by-ransomware-attack-guest-ssns-compromised/> (last accessed Sept. 24, 2024).

1 would protect that PII. Plaintiff and Class Members provided their PII to Riverside with the reasonable  
 2 expectation and mutual understanding that Riverside, and anyone Riverside contracted with, would  
 3 comply with their obligations to keep such information confidential and secure from unauthorized  
 4 access.

5 37. Riverside's data security obligations were particularly important, and Riverside is or  
 6 should be acutely aware of and understand the importance of keeping customer's PII safe, and is or  
 7 should be acutely if not uniquely aware of the given the substantial increase in cyberattacks and/or  
 8 data breaches of major companies before the Data Breach, including in the U.S. gaming industry.<sup>10</sup>  
 9

10 38. Defendants knew or should have known that these attacks were common and  
 11 foreseeable, given the rapid increase in such incidents just over the last several years. The number of  
 12 data breaches in the U.S. has significantly increased, from a mere 447 in 2012 to more than 3,200 in  
 13 2023 (Statista). The 2023 breaches included massive cyberattacks at gaming giants MGM Resorts  
 14 International and Caesars Entertainment in late 2023, involving tens of thousands of compromised  
 15 records and millions of dollars in losses.<sup>11</sup>  
 16

17 39. The increase in such attacks, and the resulting risk of future attacks, was widely known  
 18 to the public and foreseeable to anyone in the gaming industry, including Riverside.

19 40. Due to Defendants' inadequate and insufficient data security measures, Plaintiff and  
 20 Class Members now face a substantially increased risk of fraud and identity theft and must essentially  
 21

22 <sup>10</sup> See, e.g., Casino.org, 9-13-2024 "*Laughlin's Riverside Resort Casino Confirms Data Breach, 55K*  
 23 *Customers Affected*" *supra* at footnote \_\_ (last accessed Sept. 24, 2024). See also Oct. 19, 2023  
 24 Sangfor Technologies blog, *Casino Hack: Las Vegas MGM Cyber Attack*, at  
<https://www.sangfor.com/blog/cybersecurity/casino-hack-las-vegas-mgm-cyber-attack> (last  
 25 accessed Sept. 24, 2024).

26 <sup>11</sup> See *Id.*; see also *Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023), at  
 27 <https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/> (last  
 28 accessed Sept. 24, 2024).

live with that threat for the foreseeable future, if not forever. For example, Plaintiff has reported experiencing an increase of spam emails in recent months. PII stolen in incidents such as this Data Breach that comes in the hands of cybercriminals to be sold on the Dark Web has a heightened likelihood of being misused for sinister purposes. This is a common modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties, and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

42. Defendants had, and continue to have, obligations created by contract, industry standards, federal law, common law, and representations made to Plaintiff and other Class Members, to keep their valuable PII confidential and to protect it from unauthorized access and disclosure

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their PII.

44. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access and disclosure.

B. **FTC Security Guidelines Concerning PII**

45. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendants. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

46. In 2016, the FTC provided updated security guidelines in a publication titled

1 Protecting Personal Information: A Guide for Business. Under these guidelines, companies should  
2 protect consumer information they keep; limit the sensitive consumer information they keep; encrypt  
3 sensitive information sent to third parties or stored on computer networks; identify and understand  
4 network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention  
5 to the security of web applications (the software used to inform visitors to a company's website and to  
6 retrieve information from the visitors).

7  
8 47. The FTC recommends that businesses do not maintain payment card  
9 information beyond the time needed to process a transaction; restrict employee access to  
10 sensitive customer information; require strong passwords be used by employees with access to  
11 sensitive customer information; apply security measures that have proven successful in the  
12 industry; and verify that third parties with access to sensitive information use reasonable security  
13 measures.

14  
15 48. The FTC also recommends that companies use an intrusion detection system to  
16 immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a  
17 hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from  
18 the system; and develop a plan to respond effectively to a data breach in the event one occurs.

19  
20 49. The FTC has brought several actions to enforce Section 5 of the FTC Act. According  
21 to the FTC's website, the FTC can and does take law enforcement action to make sure that  
22 companies live up to their promises to consumers to safeguard their personal information. The  
23 FTC has brought legal actions against organizations that have violated consumers' privacy rights  
24 or misled them by failing to maintain security for sensitive consumer information or caused  
25 substantial consumer injury.

26  
27 50. In many of these cases, the FTC has charged the defendants with violating FTC Act  
28 Section 5, which bars unfair and deceptive acts and practices in or affecting commerce. In addition  
to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and

1 security.<sup>16</sup>

2 51. Defendants were aware or should have been aware of their obligations to protect clients'  
3 customers' PII and privacy before and during the Data Breach yet failed to take reasonable  
4 steps to protect customers from unauthorized access. Among other violations, Defendants violated  
5 their obligations under Section 5 of the FTC Act.

6 **C. Defendant Did Not Use Reasonable Security Procedures**

7  
8 52. Despite this knowledge, Defendant did not use reasonable security procedures and  
9 practices appropriate to the nature of the sensitive, non-encrypted, and non-redacted information  
10 it was maintaining for Plaintiff and Class Members, causing Plaintiff and Class Members' PII to  
11 be exposed and exfiltrated by cyber criminals.

12 53. To prevent and detect cyber-attacks, Riverside could and should have  
13 implemented, as recommended by the U. S. Government, the following measures:

- 14 ☐ Implement an awareness and training program. Because end users are
- 15 targets, employees and individuals should be aware of the threat of ransomware
- 16 and how it is delivered.
- 17 ☐ Configure firewalls to block access to known malicious IP addresses.
- 18 ☐ Patch operating systems, software, and firmware on devices. Consider
- 19 using a centralized patch management system.
- 20 ☐ Set anti-virus and anti-malware programs to conduct regular scans
- 21 automatically.
- 22 ☐ Manage the use of privileged accounts based on the principle of least
- 23 privilege: no users should be assigned administrative access unless absolutely
- 24 needed; and those with a need for administrator accounts should only use them
- 25 when necessary.
- 26 ☐ Configure access controls—including file, directory and network
- 27
- 28

1 share permissions—with least privilege in mind. If a user only needs to read  
2 specific files, the user should not have written access to those files, directories,  
3 or shares.

4 ☐ Disable macro scripts from office files transmitted via email. Consider  
5 using Office Viewer software to open Microsoft Office files transmitted via  
6 email instead of full Office Suite applications.

7 ☐ Implement Software Restriction Policies (SRP) or other controls to  
8 prevent programs from executing from common ransomware locations, such as  
9 temporary folders supporting popular Internet browsers or  
10 compression/decompression programs, including the AppData/LocalAppData  
11 folder.

12 ☐ Consider disabling the Remote Desktop Protocol (RDP) if it is not being  
13 used.

14 ☐ Use application whitelisting, which only allows systems to execute programs  
15 known and permitted by security policy.

16 ☐ Execute operating system environments or specific programs in a  
17 virtualized environment.

18 ☐ Categorize data based on organizational value and implement physical and  
19 logical separation of networks and data for different organizational units.

20  
21  
22 54. To prevent and detect cyber-attacks, Defendants could and should have  
23 implemented, as recommended by the U.S. Cybersecurity & Infrastructure Security Agency, the  
24 following measures:

25 ☐ Update and patch your computer. Ensure your applications and operating  
26 systems (OSs) have been updated with the latest patches. Vulnerable  
27 applications and OSs are the target of most ransomware attacks.  
28

□ Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters and keep them updated to reduce malicious network traffic.<sup>12</sup>

55. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit
- Remove privileged credentials
- Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise.
- Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.

**Build credential hygiene**

---

<sup>12</sup> See Cybersecurity & Infrastructure Security Agency, *Protecting Against Ransomware* (orig. Rel. date Apr. 11, 2019), at: <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last accessed Sept. 24, 2024).

-Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

**Apply principle of least-privilege**

-Monitor for adversarial activities  
 -Hunt for brute force attempts  
 - Monitor for cleanup of Event Logs  
 -Analyze logon events

**Harden infrastructure**

- Use Windows Defender Firewall  
 -Enable tamper protection  
 -Enable cloud-delivered protection  
 -Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>13</sup>

56. Given that Defendants were storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all the above measures to prevent and detect cyber-attacks.

57. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent “hacking” attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

---

<sup>13</sup> See *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed Sept. 24, 2024).

**D. Securing PII and Preventing Breaches**

58. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- A. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- D. Failing to adequately protect customers' PII;
- E. Failing to properly monitor its own data security systems for existing intrusions;
- F. Failing to ensure that it, and its vendors with access to its computer systems and data, employed reasonable security procedures; and;
- G. Failing to adhere to industry standards for cybersecurity.

59. Defendants could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data that was no longer useful, especially outdated data.

60. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members was exacerbated by the repeated warnings and alerts directed to businesses to protect and secure sensitive data. Despite the prevalence of public announcements of data breaches and data security compromises, including Defendants' own recent data breach, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

**E. Defendant Failed to Comply with Industry Standards**

61. Several best practices have been identified that, at a minimum, should be implemented by companies like Defendants, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software;

1 encryption, making data unreadable without a key; multi-factor authentication; backup data; and  
2 limiting which employees can access sensitive data. Defendants failed to follow these industry best  
3 practices.

4 62. Other best cybersecurity practices include installing appropriate malware  
5 detection software; monitoring and limiting the network ports; protecting web browsers and email  
6 management systems; setting up network systems such as firewalls, switches, and routers;  
7 monitoring and protecting physical security systems; protecting against any possible  
8 communication system; training staff regarding critical points. Defendants failed to follow these  
9 cybersecurity best practices, including failure to train staff.

11 **F. Value of Personally Identifiable Information**

12 63. The PII of individuals remains of high value to criminals, as evidenced by the prices  
13 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity  
14 credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details have  
15 a price range of \$50 to \$200.<sup>19</sup> Experian reports that a stolen credit or debit card number can sell  
16 for \$5 to \$110 on the dark web.<sup>20</sup> Criminals can also purchase access to entire company data  
17 breaches from \$900 to \$4,500.<sup>21</sup>

19 64. Social Security numbers, for example, are among the worst kind of PII to have been  
20 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual  
21 to change. The Social Security Administration stresses that the loss of an individual's Social Security  
22 number, as is the case here, can lead to identity theft and extensive financial fraud:

23  
24 A dishonest person who has your Social Security number can use it to get other  
25 personal information about you. Identity thieves can use your number and  
26 your good credit to apply for more credit in your name. Then, they use the  
27 credit cards and don't pay the bills, it damages your credit. You may not find  
28 out that someone is using your number until you're turned down for credit, or

1           you begin to get calls from unknown creditors demanding payment for  
2           items you never bought. Someone illegally using your Social Security  
3           number and assuming your identity can cause a lot of problems.<sup>[14]</sup>

4           65. Moreover, it is no easy task to change or cancel a stolen Social Security number. An  
5           individual cannot obtain a new Social Security number without significant paperwork and evidence  
6           of actual misuse. In other words, preventive action to defend against the possibility of misuse of a  
7           Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud  
8           activity to obtain a new number.

9  
10           66. Even then, a new Social Security number may not be effective. According to Julie  
11           Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the  
12           new number very quickly to the old number, so all of that old bad information is quickly inherited into  
13           the new Social Security number.”<sup>15</sup>

14           67. Based on the foregoing, the information compromised in the Data Breach is  
15           significantly more valuable than the loss of, for example, credit card information in a retailer data  
16           breach because, there, victims can cancel or close credit and debit card accounts. The information  
17           compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to  
18           change, where it includes names and Social Security numbers.

19  
20           68. This data demands a much higher price on the black market. Martin Walter, senior  
21           director at cybersecurity firm RedSeal, explained: “Compared to credit card information, personally  
22

23  
24           <sup>14</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, at  
25           <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Sept. 24, 2024).

26           <sup>15</sup> See Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR  
27           (Feb. 9, 2015), at: [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft)  
28           has-millions-worrying-about-identity-theft (last accessed Sept. 24, 2024).

identifiable information and Social Security numbers are worth more than 10x in price on the black market.”<sup>16</sup> Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

69. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches, “law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft” and that “[f]urther, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”<sup>17</sup>

70. The PII stolen in the Data Breach has significant value, as PII is a valuable property right.<sup>18</sup> Sensitive PII can sell for as much as \$363 per record, according to the Infosec Institute.<sup>19</sup>

70. There is also an active, robust, and legitimate marketplace for PII. In 2019, the data

<sup>16</sup> See Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, at <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Sept. 24, 2024).

<sup>17</sup> See *Report to Congressional Requesters*, GAO, at 29 (June 2007), at <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Sept. 24, 2024).

<sup>18</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at \*3–4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.” (citations omitted)).

<sup>19</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), at <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed Sept. 24, 2024).

1 brokering industry was worth roughly \$200 billion.<sup>20</sup> In fact, the data marketplace is so  
 2 sophisticated that consumers can sell their non-public information directly to a data broker, who in  
 3 turn aggregates the information and provides it to marketers or app developers.<sup>21</sup> Consumers who  
 4 agree to provide their web browsing history to the Nielsen Corporation can receive up to \$60.00 a  
 5 year.<sup>22</sup>

6 71. As a result of the Data Breach at issue here, Plaintiff's and other Class Members' PII,  
 7 which has an inherent market value in both legitimate and black markets, has been damaged and  
 8 diminished by its unauthorized release to third-party actors, to whom it holds significant value.  
 9 However, this transfer of value occurred without any consideration paid to Plaintiff or other Class  
 10 Members for their valuable property, resulting in an economic loss. Moreover, the PII is now readily  
 11 available, and the rarity of Plaintiff's and Class Members' PII has been lost, thereby causing additional  
 12 loss of value.  
 13

14 72. At all relevant times, Defendants knew, or reasonably should have known, of the  
 15 importance of safeguarding the PII of Plaintiff and other Class Members, including but not limited  
 16 to name, their names and Social Security numbers, and of the foreseeable consequences that would  
 17 occur if Defendants' data security systems and networks were breached, including, specifically,  
 18 the significant costs that would be imposed on Plaintiff and other Class Members as a result of a breach  
 19 and the costs associated with being denied access to their money and financial accounts.  
 20

21 73. Plaintiff and other Class Members now face the real threat of years of constant  
 22

---

24 <sup>20</sup> See David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), at <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed Sept. 24, 2024).

25 <sup>21</sup> See, e.g., <https://datacoup.com/>; see also <https://worlddataexchange.com/about> (last accessed Sept. 24, 2024).

26 <sup>22</sup> See Computer & Mobile Panel, NIELSEN, at <https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing> (last accessed Sept. 24, 2024).

1 surveillance of their financial and personal records, monitoring, and loss of rights. For one thing,  
 2 Plaintiff experienced a noticeable uptick in spam emails in recent months. Beyond the significant  
 3 stress and anxiety the situation has caused, Plaintiff and other Class members have already devoted,  
 4 and anticipated continuing to devote, countless hours to the vigilant monitoring of their identity and  
 5 financial accounts to mitigate any potential harm. In sum, the Class is incurring and will continue to  
 6 incur such damages in addition to any fraudulent use of their PII.

7  
 8 74. Defendants were, or should have been, fully aware of the unique type and the  
 9 significant volume of data on Riverside's server(s) and computer network, amounting to  
 10 potentially tens of thousands of individuals' detailed PII, and, thus, the significant number of  
 11 individuals who would be harmed by the exposure of the unencrypted data.

12 75. The injuries to Plaintiff and other Class Members were directly and proximately  
 13 caused by Defendant's failure to implement or maintain adequate data security measures for the PII  
 14 of Class Members, including, but not limited to, failing to encrypt sensitive PII, failing to redact  
 15 sensitive PII, keeping unencrypted and unredacted sensitive PII in internet facing environments, and  
 16 failing to delete sensitive PII that Defendants had no reasonable business purpose for continuing to  
 17 maintain.  
 18

19 76. The ramifications of Defendants' failure to safeguard the PII of Plaintiff and other  
 20 Class Members are long-lasting and severe. Once PII is stolen, fraudulent use of that information and  
 21 damage to victims may continue for years.  
 22

## 23 **V. PLAINTIFF'S HANSEN'S SPECIFIC ALLEGATIONS**

24 77. Plaintiff Hansen is a long-time customer of, and has an account with, Riverside. Plaintiff  
 25 has been a customer of Riverside for the past fifteen to twenty years, and has patronized Resort's  
 26 facilities scores of times during that period, first while a resident of California and then as a resident of  
 27 Mississippi.  
 28

78. Plaintiff Hansen provided his PII, at Riverside's request, when he opened his account

1 with Defendant.

2 79. Plaintiff Hansen is very careful about sharing his sensitive Private Information. Plaintiff  
3 Hansen has never knowingly transmitted unencrypted sensitive PII over the internet or any other  
4 unsecured source.

5 80. Plaintiff Hansen first learned of the Data Breach after he received a Notice from  
6 Defendant on or around September 5, 2024, notifying him that “[o]n July 25, 2024, Riverside learned  
7 of suspicious activity in its environment” and by August 9, 2024, Riverside had “identified the persons  
8 whose sensitive information was potentially impacted.”<sup>23</sup>  
9

10 81. Upon information and belief, and according to the Notice, the PII involved in the  
11 Data Breach included, at least, Plaintiff Hansen’s name and Social Security number.

12 82. As a result of the Data Breach, Plaintiff Hansen made reasonable efforts to mitigate  
13 the impact of the Data Breach after receiving the Data Breach email, including but not limited to taking  
14 reasonable steps to research the facts and information Data Breach, reviewing credit reports, and financial  
15 account statements for any indications of actual or attempted identity theft or fraud.  
16

17 83. Plaintiff Hansen has spent multiple hours, and will continue to spend valuable time  
18 for the remainder of his life, that he otherwise would have spent on other activities, including  
19 but not limited to work and/or recreation.

20 84. As a result of the Data Breach, Plaintiff Hansen has also suffered emotional distress  
21 as a result of the release of his PII, which he believed would be protected from unauthorized  
22 access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using  
23 his PII for purposes of identity theft and/or fraud. Plaintiff Hansen is very concerned about identity  
24 theft and fraud, as well as the consequences of such identity theft and/or fraud resulting from the  
25 Riverside Data Breach.  
26

27  
28 <sup>23</sup> See *supra* ¶¶ \_\_\_\_.

1           85. As a result of the Data Breach, Plaintiff Hansen anticipates spending  
2 considerable time and money on an ongoing basis to try to mitigate and address harm caused by the  
3 Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased  
4 risk of identity theft and/or fraud for the remainder of his lifetime.

5 **A. Plaintiff's Injuries and Damages**

6           86. As a direct and proximate result of Defendant's conduct, the Plaintiff and other  
7 Class Members are presently experiencing and will continue experiencing actual harm from fraud and  
8 identity theft.

9           87. Plaintiff and other Class Members are presently experiencing substantial risk of out-of-  
10 pocket fraud losses, such as loans opened in their names, tax return fraud, utility and medical bills  
11 opened in their names, and similar types of identity theft.

12           88. Plaintiff and other Class Members face substantial risk of being targeted for future  
13 phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use  
14 that information to target such schemes more effectively to Plaintiff and other Class Members.

15           89. Plaintiff and other Class Members are also incurring and may continue incurring out- of-  
16 pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze  
17 fees, and similar costs directly or indirectly related to the Data Breach.

18           90. Plaintiff and other Class Members also suffered a loss of value of their PII when it  
19 was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized the  
20 propriety of loss of value damages in related cases.

21           91. Plaintiff and other Class Members were also damaged via benefit-of-the-bargain  
22 damages. Plaintiff and Class Members overpaid for a service than they otherwise would have, in  
23 exchange for which Defendant was supposed to provide adequate data security but was not. Part of the  
24 price Plaintiff and Class Members paid to Defendant and its affiliates was intended to be used by  
25 Defendant to fund adequate security of Defendant's computer property and protect Plaintiff's and  
26  
27  
28

1 Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for.

2 92. Plaintiff and other Class Members have spent and will continue to spend significant  
3 amounts of time monitoring their financial accounts and records for fraud and misuse.

4 93. Plaintiff and other Class Members have suffered actual injury as a direct result of the  
5 Data Breach. Many victims suffered ascertainable losses in the form of unauthorized credit card  
6 transactions, lost use of financial instruments, out-of-pocket expenses, and the value of their time  
7 reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

8 a. Finding fraudulent loans, insurance claims, tax returns, and/or  
9 government benefit claims;

10 b. Purchasing credit monitoring and identity theft prevention;

11 c. Placing "freezes" and "alerts" with credit reporting agencies;

12 d. Spending time on the phone with or at financial institutions or  
13 government agencies to dispute fraudulent charges and/or claims;

14 e. Contacting financial institutions and closing or modifying financial  
15 accounts; and/or

16 f. Closely reviewing and monitoring medical insurance accounts,  
17 bank accounts, payment card statements, and credit reports for  
18 unauthorized activity for years to come.

19 94. Moreover, Plaintiff and other Class Members have an interest in ensuring that their  
20 PII, which is believed to remain in the possession of Defendant, is protected from further  
21 breaches by the implementation of security measures and safeguards, including but not limited to,  
22 making sure that the storage of data or documents containing sensitive and confidential personal,  
23 and/or financial information is not accessible online, that access to such data is password-  
24 protected, and that such data is properly encrypted.

95. Further, as a result of Defendants' conduct, Plaintiff and other Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

96. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and other Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

## **VI. CLASS ACTION ALLEGATIONS**

97. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3). Specifically, Plaintiff proposes the following Class, subject to amendment as appropriate:

**All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").**

98. Excluded from the Class are the following individuals and/or entities: any of Defendants or Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which either or both Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

99. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

100. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3):

a. **Numerosity**. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of Class Members is unknown to Plaintiff, upon information and belief, at least tens of thousands of individuals were impacted in the Data Beach. Thus, numerosity is met.

1           b. **Commonality**. There are questions of law and fact common to the Class  
2       which predominate over any questions affecting only individual Class Members.  
3       These common questions include, without limitation:

- 4           i.     Whether Defendants engaged in the conduct alleged herein;
- 5           ii.    Whether Defendants' conduct violated the FTCA;
- 6           iii.   When Defendants learned of the Data Breach;
- 7           iv.    Whether Defendants' responses to the Data Breach was  
8           adequate;
- 9           v.     Whether Defendants unlawfully lost or disclosed Plaintiff's  
10          and Class Members' PII;
- 11          vi.    Whether Defendants failed to implement and maintain  
12          reasonable security procedures and practices appropriate to the  
13          nature and scope of the PII compromised in the Data Breach;
- 14          vii.   Whether Defendants' data security systems prior to and  
15          during the Data Breach complied with applicable data security laws  
16          and regulations;
- 17          viii.   Whether Defendants' data security systems prior to and  
18          during the Data Breach were consistent with industry standards;
- 19          ix.    Whether Defendants owed duties to Plaintiff and other  
20          Class Members to safeguard their PII;
- 21          x.     Whether Defendants breached their duty to Plaintiff and  
22          other Class Members to safeguard their PII;
- 23          xi.    Whether hackers obtained Plaintiff's and other Class Members'  
24          PII via the Data Breach;
- 25          xii.   Whether Defendants had a legal duty to provide timely and  
26          adequate notice to Plaintiff and other Class Members of the Data Breach;
- 27          xiii.   Whether Defendants had a legal duty to provide timely and  
28          adequate notice to Plaintiff and other Class Members of the Data Breach;

1 accurate notice of the Data Breach to Plaintiff and other Class  
2 Members;

3 xiii. Whether Defendants breached their duties to provide timely and  
4 accurate notice of the Data Breach to Plaintiff and Class Members;

5 xiv. Whether Defendants knew or should have known that their  
6 data security systems and monitoring processes were deficient;

7 xv. What damages Plaintiff and other Class Members suffered  
8 as a result of Defendants' misconduct;

9 xvi. Whether Defendants conduct was negligent;

10 xvii. Whether Defendants unjustly enriched;

11 xviii. Whether Plaintiff and Class Members are entitled to actual  
12 and/or statutory damages;

13 xix. Whether Plaintiff and Class Members are entitled to  
14 additional credit or identity monitoring and monetary relief; and

15 xx. Whether Plaintiff and Class Members are entitled to equitable  
16 relief, including injunctive relief, restitution, disgorgement, and/or  
17 the establishment of a constructive trust.  
18

19  
20 c. **Typicality.** Plaintiff's claims are typical of those of other Class Members  
21 because Plaintiff's PII, like that of every other Class Member, was compromised in the Data  
22 Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*,  
23 all Class Members were injured through the common misconduct of Defendants. Plaintiff  
24 is advancing the same claims and legal theories on behalf of himself and all other Class  
25 Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and  
26 those of Class Members arise from the same operative facts and are based on the same legal  
27 theories.  
28

1           d.       **Adequacy of Representation.** Plaintiff will fairly and adequately represent  
2 and protect the interests of Class Members. Plaintiff's counsel is competent and  
3 experienced in litigating class actions, including data privacy litigation of this kind.

4           e.       **Predominance.** Defendant have engaged in a common course of conduct  
5 toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was  
6 stored on its computer systems and unlawfully accessed and exfiltrated in the same way. The  
7 common issues arising from Defendants' conduct affecting Class Members set out above  
8 predominate over any individualized issues. Adjudication of these common issues in a single  
9 action has important and desirable advantages of judicial economy.

10           f.       **Superiority.** A class action is superior to other available methods for the  
11 fair and efficient adjudication of this controversy and no unusual difficulties are likely  
12 to be encountered in the management of this class action. Class treatment of common questions  
13 of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class  
14 action, most Class Members would likely find that the cost of litigating their individual  
15 claims is prohibitively high and would therefore have no effective remedy. The prosecution  
16 of separate actions by individual Class Members would create a risk of inconsistent or varying  
17 adjudications with respect to individual Class Members, which would establish incompatible  
18 standards of conduct for Defendants. In contrast, conducting this action as a class action  
19 presents far fewer management difficulties, conserves judicial resources and the parties'  
20 resources, and protects the rights of each Class Member.

21           101. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have  
22 acted and/or refused to act on grounds generally applicable to the Class such that final injunctive  
23 relief and/or corresponding declaratory relief is appropriate as to the Class as a whole. Finally, all  
24 members of the proposed Class are readily ascertainable. Defendants have access to the names and  
25 addresses and/or email addresses of Class Members affected by the Data Breach. Class Members  
26  
27  
28

1 have already been preliminarily identified and sent notice of the Data Breach by Riverside.

2 **VII. CAUSES OF ACTION**

3 **FIRST CAUSE OF ACTION**

4 **Negligence**

5 **(On Behalf of Plaintiff and the Class)**

6 102. Plaintiff incorporates by reference all previous allegations as though fully set forth  
7 herein.

8 103. Defendants knowingly collected, came into possession of, and maintained and  
9 stored Plaintiff's and Class Members' PII, and had duties to exercise reasonable care in safeguarding,  
10 securing, and protecting such information from being compromised, lost, stolen, misused, and/or  
11 disclosed to unauthorized parties.

12 104. Defendants had and still have duties under common law to have procedures in place to  
13 detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

14 105. Defendants had and continue to have duties to employ reasonable security measures  
15 under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting  
16 commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use  
17 reasonable measures to protect confidential data.

18 106. Defendants' duties to use reasonable security measures required them to take reasonable  
19 and adequate measures to protect the security, confidentiality, and integrity of customer information  
20 by developing a comprehensive written information security program that contains reasonable  
21 administrative, technical, and physical safeguards.

22 107. Defendants had full knowledge of the sensitivity of the PII and the types of harm that  
23 Plaintiff and other Class Members could and would suffer if the data were wrongfully disclosed.

24 108. By assuming responsibility for collecting and storing this data, and in fact doing so and  
25 using it for commercial gain, Defendants had duties of care to use reasonable means to secure and  
26

1 safeguard Riverside's computer property—and Class Members' PII held within it—to prevent  
2 disclosure of the information, and to safeguard the information from theft. Defendants' duties  
3 include, but are not limited to, a responsibility to redact and encrypt sensitive information,  
4 promptly remove sensitive information that's no longer needed, implement processes by which it  
5 could detect a breach of its security systems in a reasonably expeditious time period, and to give  
6 prompt notice to those affected in the case of a data breach.

7  
8 109. Defendants were and are subject to "independent duties," untethered to any contract  
9 between Defendants and Plaintiff or other Class Members.

10 110. This breach of security, unauthorized access, and resulting injury to Plaintiff's and Class  
11 Members' PII was reasonably foreseeable in light of the significant increase in cyberattacks  
12 and/or data breaches of major companies before the Data Breach, including in the U.S. gaming  
13 industry.<sup>24</sup>

14 111. A breach of security, unauthorized access, and resulting injury to Plaintiff's and Class  
15 Members' PII was also reasonably foreseeable particularly considering Defendants' inadequate  
16 security practices, which include sharing and/or storing the PII of Plaintiff and Class Members on its  
17 computer systems.

18 112. Plaintiff and Class Members were the foreseeable and probable victims of such  
19 inadequate security practices and procedures, and Defendants knew or should have known of the  
20 inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical  
21 importance of providing adequate security of that data, and the necessity for encrypting all data stored  
22 on Defendants' systems.

23 113. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class  
24 Members. Defendants' misconduct included, but was not limited to, its failure to take the adequate or  
25

26  
27  
28 

---

<sup>24</sup> See *supra* ¶ \_\_ and footnote \_\_.

1 necessary steps and opportunities to prevent the Data Breach as set forth herein. Defendants'  
2 misconduct also included its decisions not to comply with state and federal law or industry standards  
3 for the safekeeping of the PII of the Plaintiff and other Class Members, including basic encryption  
4 techniques freely available to Defendants.

5 114. Plaintiff and other Class Members had no ability to protect their PII that was in, and  
6 probably remains in, Defendants' possession.

7 115. Defendants, on the other hand, were able to protect against the Data Breach and the  
8 harm suffered by Plaintiff and Class Members as a result of the Breach, but failed to do so as a result  
9 of their neglect and failure to take adequate or necessary measures to safeguard and maintain the  
10 confidentiality of the PII of the Plaintiff and other Class Members.

11 116. Defendants had and continue to have duties to adequately disclose that the PII of  
12 Plaintiff and Class Members within Defendants' possession might have been compromised, how it  
13 was compromised, and precisely the types of data that were compromised and when. Such notice was  
14 necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity  
15 theft and the fraudulent use of their PII by third parties.

16 117. Defendants have and still have duties to comply with the laws and industry  
17 standards set out above.

18 118. Defendants, through their actions and/or omissions, unlawfully breached their duties to  
19 Plaintiff and Class Members by failing to exercise reasonable care in protecting and  
20 safeguarding Plaintiff's and other Class Members' PII within Defendant's possession.

21 119. Defendants, through their actions and/or omissions, unlawfully breached their duties  
22 to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent  
23 dissemination of Plaintiff's and Class Members' PII.

24 120. Defendants, through their actions and/or omissions, unlawfully breached their duties  
25 to timely disclose to Plaintiff and Class Members that the PII within Defendants' possession might  
26

1 have been compromised and precisely the type of information compromised.

2 121. Defendants' breaches of their duties owed to Plaintiff and Class Members caused  
3 Plaintiff's and Class Members' PII to be compromised.

4 122. Defendants breached their duties, pursuant to the FTC Act, and other applicable  
5 standards, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and  
6 Class Members' PII. The specific negligent acts and omissions committed by Riverside include, but  
7 are not limited to, the following:

- 8 a. Failing to adopt, implement, and maintain adequate security  
9 measures to safeguard Plaintiff's and Class Members' PII;
- 10 b. Failing to adequately monitor the security of its networks and  
11 systems;
- 12 c. Failing to audit, monitor, or ensure the integrity of its data security  
13 practices;
- 14 d. Allowing unauthorized access to Plaintiff's and Class Members' PII;
- 15 e. Failing to detect in a timely manner that Plaintiff's and Class  
16 Members' PII had been compromised;
- 17 f. Failing to remove former customers' PII they was no longer required  
18 to retain pursuant to regulations; and
- 19 g. Failing to timely and adequately notify Plaintiff and Class  
20 Members about the Data Breach's occurrence and scope, so that they  
21 could take appropriate steps to mitigate the potential for identity theft  
22 and other damages.

23  
24  
25  
26 123. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures  
27 to protect PII and not complying with applicable industry standards, as described in detail herein.  
28 Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained

1 and stored and the foreseeable consequences of the immense damages that would result to Plaintiff  
2 and the Class.

3 124. Plaintiff and Class Members were within the class of persons the FTC Act is intended  
4 to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes  
5 were intended to guard against.

6 125. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

7 126. The FTC has pursued enforcement actions against businesses like Defendants, which,  
8 as a result of their failure to employ reasonable data security measures and avoid unfair and  
9 deceptive practices, have caused the same harm as that suffered by Plaintiff and the Class as a result of  
10 Defendants' actions and omissions here in connection with the Data Breach.

11 127. As a result of Defendants' prior and ongoing failures to notify Plaintiff and Class Members  
12 regarding the type of PII that has been compromised, Plaintiff and Class Members are unable to take  
13 the necessary precautions to mitigate damages by preventing future fraud.  
14

15 128. Defendants' breaches of their duties caused Plaintiff and Class Members to suffer from  
16 identity theft, fraud, loss of time and money to monitor their finances for fraud, loss of access to their  
17 money and financial accounts, and loss of control over their PII, and the significant additional distress  
18 and anxiety that is inevitably associated with these difficult and stressful circumstances.  
19

20 129. As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members  
21 are in danger of present and continuing harm in that their PII, which is still in the possession of  
22 third parties, will be used for fraudulent purposes. Plaintiff and Class Members will need identity  
23 theft protection services and credit monitoring services for their respective lifetimes (well beyond one  
24 year), considering the immutable nature of the PII at issue, which Riverside has admitted includes the  
25 names and Social Security numbers of Plaintiff and other Class Members.  
26

27 130. There is a close causal connection between Defendants' failure to implement sufficient  
28 security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of

1 imminent harm, experienced by Plaintiff and other Class Members. The PII of Plaintiff and other Class  
 2 Members was stolen and accessed as the proximate result of Defendants' failure to exercise  
 3 reasonable care in safeguarding such PII, by adopting, implementing, and maintaining appropriate  
 4 security measures.

5 131. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

6 132. In failing to secure Plaintiff's and Class Members' PII and failing to promptly or  
 7 adequately notify them of the Data Breach, Defendants are also guilty of oppression, fraud, and/or  
 8 malice, in that Defendants acted or failed to act with a willful and conscious disregard of Plaintiff's  
 9 and other Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks  
 10 punitive damages on behalf of himself and the Class.  
 11

12 133. Plaintiff also seeks injunctive relief on behalf of the Class in the form of an order  
 13 compelling Defendants to institute appropriate data collection and safeguarding methods and  
 14 policies regarding customer information.  
 15

## 16 **SECOND CAUSE OF ACTION**

### 17 ***Negligence per se***

#### 18 **(On Behalf of Plaintiff and the Class)**

19 134. Plaintiff incorporates by reference all previous allegations as though fully set forth  
 20 herein.

21 135. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting  
 22 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by companies  
 23 like Defendants of failing to use adequate or reasonable measures to protect PII.  
 24

25 136. The FTC publications and orders also form the basis of Defendants' duties to the Class.

26 137. Defendants violated Section 5 of the FTC Act (and other similar state privacy statutes  
 27 requiring businesses collecting or maintaining customer personal information to implement and  
 28 maintain reasonable security measures appropriate to the nature of the information to protect it from

1 unauthorized access, use, or disclosure ) by failing to use reasonable measures to protect PII, and by  
 2 not complying with industry standards. Defendants' conduct was particularly unreasonable given the  
 3 nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach  
 4 of that data.

5 138. Defendants' violation of Section 5 of the FTC Act, similar state statutes and/or industry  
 6 standards constitutes negligence *per se*.

7 139. The Plaintiff and other Class Members are consumers within the class of persons  
 8 Section 5 of the FTC Act was intended to protect.  
 9

10 140. Moreover, the harm that has occurred is the type of harm the FTC Act and other similar  
 11 state regulations were intended to guard against. Indeed, the FTC has pursued over fifty enforcement  
 12 actions against businesses that, as a result of their failure to employ reasonable data security measures  
 13 and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

14 141. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and other  
 15 Class Members have been injured as described herein, and are entitled to damages, including  
 16 compensatory, punitive, and nominal damages, in amounts to be proven at trial.  
 17

### 18 **THIRD CAUSE OF ACTION**

#### 19 **Unjust Enrichment**

#### 20 **(On Behalf of Plaintiff and the Class)**

21 142. Plaintiff incorporates by reference all previous allegations as though fully set forth  
 22 herein.  
 23

24 143. Plaintiff and other Class Members conferred monetary benefits to Defendants by  
 25 paying Defendants, and entrusting money to Defendants, for various services relating to  
 26 Defendants' business operations at Riverside.

27 144. Defendants knew that Plaintiff and other Class Members conferred monetary benefits  
 28 to Defendants by entering into business relationships with them. Defendants acknowledged and

1 retained these benefits when they accepted the terms of these relationships with the Plaintiff and other  
2 Class Members.

3 145. Defendants were supposed to, but failed to, use a portion of the monetary benefits  
4 provided from Plaintiff and other Class Members to secure the PII belonging to Plaintiff and Class  
5 Members by paying for costs of reasonable and adequate data management and security.

6 146. Defendants should not be permitted to retain any of the monetary benefits they  
7 received as a result of their failure to implement adequate and necessary security measures to protect  
8 the safety and confidentiality PII of Plaintiff and other Class Members.

9 147. Defendants gained access to Plaintiff's and other Class Members' PII through  
10 unfair, deceptive and inequitable means because Defendants failed to disclose that they used  
11 inadequate and unreasonable security measures.

12 148. Plaintiff and other Class Members were unaware of the unreasonable and inadequate  
13 security measures and would not have provided their PII to Defendants had they known of these  
14 unreasonable and inadequate security measures.

15 149. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff  
16 and the Class Members have no adequate remedy at law.

17 150. As a direct and proximate result of Defendants' conduct, Plaintiff and the other  
18 Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;  
19 (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise and/or theft of their  
20 PII; (iv) out-of-pocket expenses associated with travel expenses and the significant efforts necessary  
21 prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their  
22 PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing  
23 and attempting to mitigate the actual and future consequences of the Data Breach, including but not  
24 limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and  
25 identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the ongoing and  
26  
27  
28

1 continued risk to their PII, which remains in Defendants' possession and is subject to further  
2 unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures  
3 to protect the PII of Plaintiff and Class Members; (viii) loss of access to their money and financial  
4 accounts; and (ix) future costs in terms of time, effort, and money that will be expended to prevent,  
5 detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the  
6 remainder of the lives of Plaintiff and Class Members.

7  
8 151. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class  
9 Members have suffered and will continue to suffer other forms of injury and/or harm, including, but  
10 not limited to, significant anxiety, emotional distress, loss of privacy, and other economic and  
11 non-economic losses.

12 152. Defendants should be compelled to disgorge into a common fund or constructive trust,  
13 for the benefit of the Plaintiff and other Class Members, all proceeds from the monetary benefits that  
14 Defendants unjustly received from them.

#### 15 16 **FOURTH CAUSE OF ACTION**

##### 17 **Breach of Implied Contract**

##### 18 **(On Behalf of Plaintiff and the Class)**

19 153. Plaintiff incorporates by reference all previous allegations as though fully set forth  
20 herein.

21 154. Plaintiff and the Class, encompassing clients, customers, business relations, and  
22 claimants of the Defendants, delivered their PII to Defendants as part of the process of engaging in  
23 certain business and related transactions.

24  
25 155. Upon providing their PII in exchange for professional or other goods and/or services,  
26 or other transactions, Plaintiff and other Class Members entered into implied contracts with  
27 Defendants under which Defendants agreed to safeguard and protect such information and also to  
28 promptly, timely, accurately and thoroughly notify Plaintiff and other Class Members that their PII had

1 been breached and compromised.

2 156. Each such contractual relationship imposed on Defendants an implied covenant of  
3 good faith and fair dealing by which Defendants were required to perform their obligations and  
4 manage Plaintiff's and Class Member's data in ways comporting with the reasonable expectations of  
5 security, privacy, confidentiality and protection attendant to entrusting such sensitive and valuable data  
6 to the Defendants.

7 157. In providing their PII, Plaintiff and other Class Members entered into an implied  
8 contract with Defendants whereby the latter, in receiving such data, became obligated to  
9 reasonably and adequately safeguard Plaintiff's and the other Class Members' PII.  
10

11 158. In delivering their PII to Defendants, Plaintiff and Class Members intended and  
12 understood that Defendants would take reasonable and adequate steps to safeguard that data.

13 159. Plaintiff and the Class Members would not have entrusted their PII to Defendants in the  
14 absence of such an implied contract.

15 160. Defendants accepted possession of Plaintiff's and Class Members' personal data for  
16 the purpose of providing certain goods and services to Plaintiff and Class Members, from which  
17 Defendants derived substantial profits.  
18

19 161. Had Defendant disclosed to Plaintiff and Class Members that Defendants did not have  
20 adequate computer systems and security practices to secure PII, Plaintiff and members of the Class  
21 would not have provided their PII to Defendants.

22 162. Defendants recognized that the PII at issue is highly sensitive and valuable and must be  
23 adequately protected, and that such protection was of material importance as part of their bargain  
24 with Plaintiff and Class Members.  
25

26 163. Plaintiff and the other Class fully performed their obligations under the implied  
27 contracts with Defendants.

28 164. Defendants breached the implied contracts with Plaintiff and Class Members by

1 failing to take reasonable and adequate measures to safeguard their data.

2 165. Defendants breached the implied contract with Plaintiff and Class Members by failing  
3 to promptly, adequately or thoroughly notify them of the unlawful and unauthorized access to and  
4 acquisition of their sensitive and valuable PII.

5 166. As a direct and proximate result of the breach of the contractual duties, Plaintiff and  
6 other Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by  
7 Plaintiff and the other Class Members include: (a) the invasion of privacy; (b) the compromise,  
8 disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs  
9 associated with the time spent to detect and prevent identity theft, including loss of productivity; (d)  
10 monetary costs associated with the detection and prevention of identity theft; (e) economic costs,  
11 including time and money, related to incidents of actual identity theft; (f) the emotional distress,  
12 fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g)  
13 the diminution in the value of the services bargained for as Plaintiff and Class Members were  
14 deprived of the data protection and security that Defendants promised when Plaintiff and the  
15 other Class Members entrusted Defendants with their PII; (h) loss of access to their accounts; and  
16 (i) the continued and substantial risk to Plaintiff's and Class Members' PII, which upon information  
17 and belief has not only been improperly compromised and disclosed and distributed to unauthorized  
18 third parties, but remains in the Defendants' possession and subject to inadequate safety, security  
19 and protection measures.

## 22 **FIFTH CAUSE OF ACTION**

### 23 **Violation of the Nevada Consumer Fraud Act**

24 **Nev. Rev. Stat. § 41.600**

25 **(On Behalf of Plaintiff and the Class)**

26 167. Plaintiffs restate and reallege all preceding factual allegations as if fully set forth herein.

27 168. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part, that  
28

1 an action may be brought by any person who is a victim of consumer fraud.

2 169. As used in this section, “consumer fraud” means: . . . A deceptive trade practice  
3 defined in NRS 598.0915 to 598.0225, inclusive. NRS § 41.600(1) & (2)(e). The Nevada Consumer  
4 Fraud Act further provides, at NRS § 598.0923(2), that “[a] person engages in a ‘deceptive trade  
5 practice’ when in the course of his or her business or occupation he or she knowingly . . . [f]ails  
6 to disclose a material fact in connection with the sale or lease of goods or services.” *Id.*

7 170. Defendants violated this provision in failing to disclose the material fact that their data  
8 security measures were inadequate to reasonably safeguard customers’ PII. Among other things,  
9 Riverside knew or should have known of the substantial risks of cyberattacks such as the Data  
10 Breach, and Defendants knew or should have known that their data security measures were  
11 insufficient to guard against attacks such as the Data Breach at issue herein. Defendants had  
12 knowledge of the facts that constituted the omissions, and could have and should have made  
13 proper disclosures to the Plaintiff and other Class Members prior to offering and providing services  
14 to those customers by any other means reasonably calculated to inform customers of its unreasonable  
15 and inadequate data security measures.

16 171. Under NRS § 598.0923(3) “[a] person engages in a ‘deceptive trade practice’ when in  
17 the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal  
18 statute or regulation relating to the sale or lease of goods or services.” *Id.* Defendants violated this  
19 provision in multiple different respects, each an independent basis for a violation of the statute.

20 172. Defendants breached their duties under NRS § 603A.210, *Security and Privacy of*  
21 *Personal Information*, which requires any data collector “that maintains records which contain  
22 personal information” of Nevada residents to “implement and maintain reasonable security measures  
23 to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure.”  
24 *Id.* Defendants are “data collector[s]” as defined by NRS § 603A.030, and they failed to implement  
25 such reasonable security measures, as shown by a system-wide breach of its computer systems during  
26  
27  
28

1 which a threat actor exfiltrated customer PII. Defendants' violation of this statute was knowing  
2 for purposes of the Nevada Consumer Fraud Statute, NRS § 598.0923(3) because they knew or should  
3 have known that they would be a target of cyberattacks such as the Data Breach.

4 173. Defendants knew or should have known that their data security measures were  
5 inadequate to protect against cyberattacks such as the Data Breach.

6 174. Riverside also violated Section 5 of the FTC Act, as alleged above, because they  
7 knew or should have known that their data security measures were unreasonable inadequate, and  
8 failed to adhere to the FTC's data security guidance. Defendants were well aware that the casino  
9 industry is a frequent target of cyberattacks such as the Breach, and this is also true because the FTC  
10 has recommended various data security measures that companies like Defendants could and should  
11 implement to mitigate the risk of a Data Breach.

12 175. Defendants chose not to follow such guidance and knew/should have known that  
13 their data security measures were inadequate to guard against cyberattacks such as the Data Breach.  
14 Defendants had knowledge of the facts that constituted the violation. Defendants' violation of Section  
15 5 of the FTC Act serves as a separate actional basis for purposes of violating NRS § 598.0923(3).

16 176. Defendants engaged in an unfair practice by engaging in conduct that is contrary to  
17 public policy, unscrupulous, and caused injury to Plaintiff and other Class Members.

18 177. As a result of these violations, Plaintiff and other Class Members are entitled to an award  
19 of actual damages, equitable injunctive relief requiring Defendants to implement adequate data  
20 security measures, as well as an award of reasonable attorney's fees and costs. NRS § 41.600(3).

## 21 **SIXTH CAUSE OF ACTION**

### 22 **Declaratory Judgment**

#### 23 **(On Behalf of Plaintiff and the Class)**

24 178. Plaintiff restates and realleges all preceding allegations set forth above as if fully  
25 alleged herein.

1           179. Under the Federal Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this  
2 Court is authorized to enter a judgment declaring the rights and legal relations of the parties and  
3 grant necessary relief. Under the Declaratory Judgment Act the Court has broad authority to restrain  
4 tortious acts, such as here, that violate the terms of the federal and state laws described in this  
5 Complaint.

6           180. An actual controversy exists as a result of the Data Breach at issue herein in  
7 which Plaintiff's and Class Members' PII has been compromised, and whether Defendants  
8 currently maintain data security measures adequate to protect Plaintiff and Class Members from  
9 further such breaches. Plaintiff alleges that Defendants' data security measures remain inadequate.  
10 Additionally, Plaintiff and other Class members continues to suffer injury as a result of the  
11 compromise their PII and remains at imminent risk that further compromises of their PII will occur  
12 in the future.

13  
14           181. Pursuant to its authority under the Federal Declaratory Judgment Act, the Court  
15 should enter a judgment declaring that, among other things:

- 16  
17                   a. Defendants owed legal duties to secure customers' PII under the  
18 common law, Section 5 of the FTC Act, and state data security laws; and  
19  
20                   b. Defendants breached and continue to breach their legal duty by  
21 failing to employ reasonable measures to secure customers' PII.

22           182. This Court also should issue corresponding prospective injunctive relief requiring  
23 Defendants to employ adequate security protocols consistent with law and industry standards to  
24 protect members' PII.

25           183. If an injunction is not issued, Plaintiff and other Class Members will suffer  
26 irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Riverside.  
27 The risk of another such breach is real, immediate, and substantial. If another breach at Riverside  
28

occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and Class Members will be forced to bring multiple lawsuits to rectify the same conduct.

184. The hardship to Plaintiff and the other Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

185. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another such data breach that compromises the valuable confidential PII.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiff and his counsel to represent the Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff, other Class Members, and the public at large including but not limited to an order:
  - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and state or local laws;

- 1                   iii.     requiring Defendants to delete, destroy, and purge the PII of  
2                   Plaintiff, other Class Members, and all members of the public  
3                   whose PII Defendants retain or may retain in the future unless  
4                   Defendants can provide to the Court reasonable justification for the  
5                   retention and use of such information when weighed against the  
6                   privacy interests of Plaintiff, other Class Members, and the public  
7                   at large;
- 8                   iv.     requiring Defendants to provide out-of-pocket expenses associated  
9                   with the prevention, detection, and recovery from identity theft, tax  
10                  fraud, and/or unauthorized use of their PII for Plaintiff's and other  
11                  Class Members' respective lifetimes;
- 12                  v.     requiring Defendants to implement and maintain a comprehensive  
13                  Information Security Program designed to protect the  
14                  confidentiality and integrity of the PII of Plaintiff, other Class  
15                  Members, and any member of the public at large whose PII  
16                  Defendants possess, or may come to possess, in the future;
- 17                  vi.    prohibiting Defendants from maintaining the PII of Plaintiff, Class  
18                  Members, and any member of the public at large whose PII  
19                  Defendants possess, or may come to possess, in the future on a  
20                  cloud-based database;
- 21                  vii.   requiring Defendants to engage independent third-party security  
22                  auditors/penetration testers as well as internal security personnel to  
23                  conduct testing, including simulated attacks, penetration tests, and  
24                  audits on Defendants' systems on a periodic basis, and ordering  
25                  Defendants to promptly correct any problems or issues detected by  
26                  such third-party security auditors;
- 27                  viii.   requiring Defendants to engage independent third-party security  
28                  auditors and internal personnel to run automated security  
                  monitoring;
- ix.    requiring Defendants to audit, test, and train security personnel  
                  regarding any new or modified procedures;
- x.     requiring Defendants to segment data by, among other things,  
                  creating firewalls and controls so that if one area of Defendants'

1 networks are compromised, hackers cannot gain access to portions  
2 of Defendants' systems;

3 xi. requiring Defendants to conduct regular database scanning and  
4 securing checks;

5 xii. requiring Defendants to establish an information security training  
6 program that includes at least annual information security training  
7 for all employees, with additional training to be provided as  
8 appropriate based upon the employees' respective responsibilities  
9 with handling personal identifying information, as well as  
10 protecting the personal identifying information of Plaintiff, other  
11 Class Members, and any member of the public at large whose PII  
12 Defendants possess, or may come to possess, in the future;

13 xiii. requiring Defendants to routinely and continually conduct internal  
14 training and education, and on an annual basis to inform internal  
15 security personnel how to identify and contain a breach when it  
16 occurs and what to do in response to a breach;

17 xiv. requiring Defendants to implement a system of tests to assess  
18 employees' knowledge of the education programs discussed in the  
19 preceding subparagraphs, as well as randomly and periodically  
20 testing employees' compliance with Defendants' policies,  
21 programs, and systems for protecting personal identifying  
22 information;

23 xv. requiring Defendants to implement, maintain, regularly review, and  
24 revise as necessary a threat management program designed to  
25 appropriately monitor Defendants' information networks for  
26 threats, both internal and external, and assess whether monitoring  
27 tools are appropriately configured, tested, and updated;

28 xvi. requiring Defendants to meaningfully educate all Class Members  
about the threats that they face as a result of the loss of their  
confidential personal identifying information to third parties, as  
well as the steps affected individuals must take to protect  
themselves;

xvii. requiring Defendants to implement logging and monitoring  
programs sufficient to track traffic to and from Defendants' servers;  
and for a period of 10 years, appointing a qualified and independent

1 third party assessor to conduct a SOC 2 Type 2 attestation on an  
2 annual basis to evaluate Defendants' compliance with the terms of  
3 the Court's final judgment, to provide such report to the Court and  
4 counsel for the class, and to report any deficiencies with such  
5 compliance;

6 D. For an award of damages, including actual, nominal, statutory, treble, consequential, and  
7 punitive damages, as allowed by law in an amount to be determined;

8 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

9 F. For prejudgment interest on all amounts awarded; and

10 G. Such other and further relief as this Court may deem just and proper

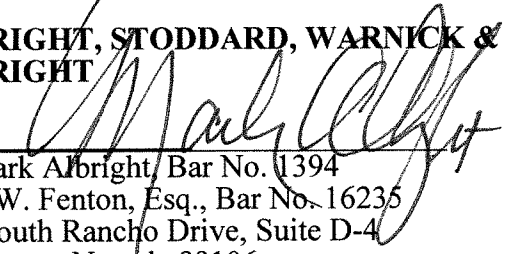
11 **DEMAND FOR JURY TRIAL**

12 Plaintiff hereby demands that this matter be tried before a jury.

13 DATED this 27<sup>th</sup> day of September, 2024

14 Respectfully submitted,

15 **ALBRIGHT, STODDARD, WARNICK &**  
16 **ALBRIGHT**

17 By:   
18 G. Mark Albright, Bar No. 1394  
19 Kyle W. Fenton, Esq., Bar No. 16235  
20 801 South Rancho Drive, Suite D-4  
21 Las Vegas, Nevada 89106  
22 Telephone: (702) 384-7111  
23 Facsimile: (702) 384-0605  
24 Email: [gma@albrightstoddard.com](mailto:gma@albrightstoddard.com)  
25 [kfenton@albrightstoddard.com](mailto:kfenton@albrightstoddard.com)

26 **WOLF HALDENSTEIN ADLER**  
27 **FREEMAN & HERZ LLP**  
28 Carl Malmstrom, Esq. (*pro hac vice forthcoming*)  
One South Dearborn Street, Suite 2122  
Chicago, IL 60603  
Telephone: (312) 984-0000  
Facsimile: (212) 686-0114  
Email: [malmstrom@whafh.com](mailto:malmstrom@whafh.com)

**BRONSON LEGAL LLC**

Kent A. Bronson, Esq. (*pro hac vice forthcoming*)

1216 Broadway, 2<sup>nd</sup> Floor

New York, NY 10001

Telephone: (212) 594-5300

Facsimile: (212) 868-1229

Email: [bronsonlegalny@gmail.com](mailto:bronsonlegalny@gmail.com)

*Attorneys for Plaintiff and the Proposed Class*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28